

IEEE P1363a / D2 (Draft Version 2)

Standard Specifications for Public Key Cryptography: Pintsov-Vanstone Signatures with Message Recovery

Abstract. This document contains possible additions to IEEE 1363a / D1, namely inclusion of a signature scheme with partial message recovery due to Pintsov and Vanstone.

6	PRIMITIVES BASED ON THE DISCRETE LOGARITHM PROBLEM.....	2
6.2	PRIMITIVES.....	2
6.2.9	DLSP-PVSSR (new for D2).....	2
6.2.10	DLRP-PVSSR (new for D2).....	3
7	PRIMITIVES BASED ON THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM .	4
7.2	PRIMITIVES.....	4
7.2.9	ECSP-PVSSR (new for D2).....	4
7.2.10	ECRP-PVSSR (new for D2).....	5
10	SIGNATURE SCHEMES.....	6
10.5	DL/ECPVSSR (NEW FOR D2).....	6
10.5.1	Scheme Options (new for D2).....	7
10.5.2	Signature Generation Operation (new for D2).....	7
10.5.3	Signature Verification (and Recovery) Operation (new for D2).....	7
12	MESSAGE ENCODING METHODS	8
12.3	MESSAGE ENCODING METHODS FOR SIGNATURES WITH MESSAGE RECOVERY.....	8
12.3.2	EMSR2 (new for D2).....	8
12.4	MESSAGE DIVISION METHODS FOR SIGNATURES WITH MESSAGE RECOVERY.....	9
12.4.1	DMSR1 (new for D2).....	9

6 Primitives Based on the Discrete Logarithm Problem

6.2 Primitives

6.2.9 DLSP-PVSSR (new for D2)

DLSP-PVSSR is Discrete Logarithm Signature Primitive, PVSSR (recovery) version. It is based on the work of [PV99]. It can be invoked in a scheme DLPVSSR to compute, with the private key of the signer, a signature on a message divided into a cryptographic portion and a verification portion. The cryptographic portion of the message can be recovered from the signature with the verification portion of the message and the primitive ECRP-PVSSR.

NOTE—this primitive is meant for the scheme DLPVSSR, where some form of redundancy in the cryptographic portion of the message is necessary.

Input:

- The DL domain parameters q, r and g associated with the key s
- The signer's private key s
- An signer's identity octet-string I
- A cryptographic message portion cM
- A verification message portion vM
- A selected symmetric encryption operation, denoted by Sym , which should be XOR, DEA or AES
- A selected mask generation function, denoted by Mgf , which should be MGF1
- A selected message encoding method, which should be EMSR2
- A selected key derivation function, denoted by Kdf , which should be KDF1

Assumptions: private key s and DL domain parameters q, r and g are valid and associated with each other; the message representatives produced by the encoding operation of the selected message encoding method are compatible as plaintext of the symmetric encryption method; the key produced by the selected key derivation function should be compatible with the selected symmetric encryption method

Output: the signature, which is a pair of integers (c, d) , where c is an octet string and $1 \leq d \leq r$

Operation. The signature (c, d) shall be computed by the following or an equivalent sequence of steps:

1. Generate a key pair (u, v) with the same set of domain parameters as the private key s . (See the note below.)
2. Convert v to an octet string ov with FE2OSP
3. Use the selected key derivation function, Kdf , to produce a symmetric key K from the octet string ov and key derivation parameter $P=00$ (K will be a valid symmetric key input to Sym).
4. Use the encoding operation of the selected encoding method to produce a message representative f of maximum length l from the confidential message portion cM (f will be a valid plaintext input to Sym).
5. Use Sym with symmetric key K to encrypt plaintext f into a ciphertext c .
6. Let $h = Mgf(c || I || vM)$
7. Convert h into an integer j with primitive OS2IP
8. Let $k = j \bmod r$
9. Let $d = sk + u \bmod r$
10. Output the pair (c, d) as the signature.

Conformance region recommendation: A conformance region should include:

- At least one valid set of DL domain parameters q, r and G
- At least one valid private key s for each set of domain parameters
- A range of message divided into portions cM, vM ; this should at least include all cM, vM with bit length no greater than that of r , where r is from the domain parameters of s

NOTE—The key pair in Step 1 should be a one-time key pair which is generated and stored by the signer following security recommendations of D.3.2, D.4.2.2, D.6 and D.7. A new key pair should be generated for every signature. The one-time private key u should be discarded after Step 4, as its recovery by an opponent can lead to the recovery of the private key s .

6.2.10 DLSP-PVSSR (new for D2)

DLSP-PVSSR is Discrete Logarithm Recovery Primitive, PVSSR (recovery) version. It is based on the work of [PV99]. The primitive recovers the cryptographic portion of a message from the verification portion, the signature, the signer's public key, the signer's identity and the domain parameters. It can be invoked in part of the scheme DLPVSSR.

Verification is done within the scheme DLSPVSSR, and requires a certain kind of redundancy in the recovered cryptographic portion of the message.

Input:

- The DL domain parameters q, r and g associated with the key w
- The signer's public key w
- The signer's identity octet-string I
- The signature (c, d)
- A verification message portion vM
- A selected symmetric encryption operation, denoted by Sym , which could be XOR, DEA or AES
- A selected mask generation function, denoted by Mgf , which could be MGF1
- A selected message encoding method, which could be EMSR2
- A selected key derivation function, denoted by Kdf , which should be KDF1

Assumptions: public key w and DL domain parameters q, r and g are valid and associated with each other; the message representatives produced by the encoding operation of the selected message encoding method are compatible as plaintext of the symmetric encryption method; the keys produced by the selected key derivation function should be valid as symmetric keys for the selected symmetric encryption method

Output: either the cryptographic portion of the message, which is an octet-string cM , or “invalid”.

Operation. The cryptographic portion of the message, cM , shall be computed by the following or an equivalent sequence of steps:

1. If d is not in the range $[1, r - 1]$, stop and output “invalid”
2. Let $h = \text{Mgf}(c || I || vM)$
3. Convert h into an integer j with primitive OS2IP
4. Let $k = j \bmod r$
5. Compute the field element $v = \exp(g, d) / \exp(w, k)$. (If $v = 1$, then stop and output “invalid”.)
6. Convert v to an octet string ov with FE2OSP
7. Use the selected key derivation function Kdf , to produce a symmetric key K from the octet string ov and key derivation parameter $P=00$ (K will be a valid symmetric key input to Sym).
8. Use Sym with symmetric key K to decrypt ciphertext c into a plaintext f .
9. Use the decoding operation of the selected encoding method to produce a message representative cM of maximum length l from f .
10. Output cM

Conformance region recommendation: A conformance region should include:

- At least one valid set of DL domain parameters q, r and g
- At least one valid public key w for each set of domain parameters
- All verification portions of messages vM that can be input to the implementation; this should at least include all vM with bit length no greater than that of r , where r is from the domain parameters of w
- All purported signatures (c, d) that can be input to the implementation; this should at least include all (c, d) such that c is an octet string with bit length no greater than that of r , and d is in the range $[1, r - 1]$, where r is from the domain parameters of w

NOTE— The main part of the verification, the acceptance or refusal of the signature (c, d) as authentic and legitimate is completed in the scheme that invokes this recovery primitive. The invoking scheme may require cM to have certain form and amount of redundancy, such as consisting of a minimum length encoding of English language. It is deemed unlikely, that someone different than the signer could generate a signature such that cM would have such redundancy.

7 Primitives Based on the Elliptic Curve Discrete Logarithm Problem

7.2 Primitives

7.2.9 ECSP-PVSSR (new for D2)

ECSP-PVSSR is Elliptic Curve Signature Primitive, PVSSR (recovery) version. It is based on the work of [PV99]. It can be invoked in a scheme ECPVSSR to compute, with the private key of the signer, a signature on a message divided into a cryptographic portion and a verification portion. The cryptographic portion of the message can be recovered from the signature with the verification portion of the message and the primitive ECRP-PVSSR.

NOTE—this primitive is meant for the scheme ECPVSSR, where some form of redundancy in the cryptographic portion of the message is necessary.

Input:

- The EC domain parameters q, a, b, r and G associated with the key s
- The signer's private key s
- An signer's identity octet-string I
- A cryptographic message portion cM
- A verification message portion vM
- A selected symmetric encryption operation, denoted by Sym , which could be XOR, DEA or AES
- A selected mask generation function, denoted by Mgf , which could be MGF1
- A selected message encoding method, which could be EMSR2
- A selected key derivation function, denoted by Kdf , which should be KDF1

Assumptions: private key s and EC domain parameters q, a, b, r and G are valid and associated with each other; the message representatives produced by the encoding operation of the selected message encoding method are compatible as the plaintext of the selected symmetric encryption method; the keys produced by the selected key derivation function should be compatible with the selected symmetric encryption method

Output: the signature, which is a pair of integers (c, d) , where c is an octet string and $1 \leq d \leq r$

Operation. The signature (c, d) shall be computed by the following or an equivalent sequence of steps:

1. Generate a key pair (u, V) with the same set of domain parameters as the private key s . (See the note below.)
2. Convert V to an octet string U with FE2OSP applied to each coordinate of V
3. Use the selected key derivation function, Kdf , to produce a symmetric key K from the octet string U and key derivation parameter $P=00$ (K will be a valid symmetric key input to Sym).
4. Use the encoding operation of the selected encoding method to produce a message representative f of maximum length l from the cryptographic message portion cM (f will be a valid plaintext input to Sym).
5. Use Sym with symmetric key K to encrypt plaintext f into a ciphertext c .
6. Let $h = Mgf(c || I || vM)$
7. Convert h into an integer j with primitive OS2IP
8. Let $k = j \bmod r$
9. Let $d = sk + u \bmod r$
10. Output the pair (c, d) as the signature.

Conformance region recommendation: A conformance region should include:

- At least one valid set of EC domain parameters q, a, b, r and G
- At least one valid private key s for each set of domain parameters
- A range of message divided into portions cM, vM ; this should at least include all cM, vM with bit length no greater than that of r , where r is from the domain parameters of s

NOTE—The key pair in Step 1 should be a one-time key pair which is generated and stored by the signer following security recommendations of D.3.2, D.4.2.2, D.6 and D.7. A new key pair should be generated for every signature. The one-time private key u should be discarded after Step 4, as its recovery by an opponent can lead to the recovery of the private key s .

7.2.10 ECRP-PVSSR (new for D2)

ECSP-PVSSR is Elliptic Curve Recovery Primitive, PVSSR (recovery) version. It is based on the work of [PV99]. The primitive recovers the cryptographic portion of a message from the verification portion, the signature, the signer's public key, the signer's identity and the domain parameters. It can be invoked in part of the scheme ECPVSSR.

Verification is done within the scheme ECSPVSSR, and requires a certain kind of redundancy in the recovered cryptographic portion of the message.

Input:

- The EC domain parameters q, a, b, r and G associated with the key W
- The signer's public key W
- The signer's identity octet-string I
- The signature (c, d)
- A verification message portion vM
- A selected symmetric encryption operation, denoted by Sym , which could be XOR, DEA or AES
- A selected mask generation function, denoted by Mgf , which could be MGF1
- A selected message encoding method, which could be EMSR2
- A selected key derivation function, denoted by Kdf , which should be KDF1

Assumptions: public key W and EC domain parameters q, a, b, r and G are valid and associated with each other; the message representatives produced by the encoding operation of the selected message encoding method are compatible as the plaintext of the selected symmetric encryption method; the keys produced by the selected key derivation function should be compatible with the selected symmetric encryption method

Output: either the cryptographic portion of the message, which is an octet-string cM , or "invalid".

Operation. The cryptographic portion of the message, cM , shall be computed by the following or an equivalent sequence of steps:

1. If d is not in the range $[1, r - 1]$, stop and output "invalid"
2. Let $h = Mgf(c || I || vM)$
3. Convert h into an integer j with primitive OS2IP
4. Let $k = j \bmod r$
5. Compute the elliptic curve point $V = dG - kW$. (If $V = 0$, then stop and output "invalid".)
6. Convert V to an octet string U with FE2OSP applied to each coordinate of V
7. Use the selected key derivation function, Kdf , to produce a symmetric key K from the octet string U and key derivation parameter $P=00$ (K will be a valid symmetric key input to Sym).
8. Use Sym with symmetric key K to decrypt ciphertext c into a plaintext f .
9. Use the decoding operation of the selected encoding method to produce a message representative cM of maximum length l from f .
10. Output cM

Conformance region recommendation: A conformance region should include:

- At least one valid set of EC domain parameters q, a, b, r and G
- At least one valid public key W for each set of domain parameters
- All verification portions of messages vM that can be input to the implementation; this should at least include all vM with bit length no greater than that of r , where r is from the domain parameters of W
- All purported signatures (c, d) that can be input to the implementation; this should at least include all (c, d) such that c is an octet string with bit length no greater than that of r , and d is in the range $[1, r - 1]$, where r is from the domain parameters of W

NOTE— The main part of the verification, the acceptance or refusal of the signature (c, d) as authentic and legitimate is completed in the scheme that invokes this recovery primitive. The invoking scheme may require cM to have certain form and amount of redundancy, such as consisting of a minimum length encoding of English language. It is deemed unlikely, that someone different than the signer could generate a signature such that cM would have such redundancy.

10 Signature Schemes

10.5 DL/ECPVSSR (new for D2)

DL/ECPVSSR is Discrete Logarithm and Elliptic Curve Pintsov-Vanstone Signature Scheme with Recovery.

10.5.1 Scheme Options (new for D2)

The following options shall be established or otherwise agreed upon between the parties to the scheme (the signer and the verifier):

- The signature and recovery primitives, which shall be one of the following pair of primitives:
 - The pair ECSP-PVSSR and ECRP-PVSSR, or the pair DLSP-PVSSR and DLRP-PVSSR
- The message encoding method, which should be EMSR2
- The key derivation function, which should be KDF1
- The mask generation function, which should be MGF1
- The symmetric encryption method, which should be XOR, DEA or AES
- The message division method
- The redundancy criteria (see note below).

The above information may remain the same for any number of executions of the signature scheme, or it may be changed at some frequency. The information need not be kept secret.

NOTE— The redundancy criteria should include at least 40-80 bits of redundancy, depending on the desired level of security. The exact nature of these is outside the scope of the description of the scheme here. It is recommended that the redundancy criteria occur naturally, such as in human language, machine language, name or address, or as graphics. It is also recommended that the redundancy criteria should be verifiable by an automated process.

10.5.2 Signature Generation Operation (new for D2)

A signature (c,d) shall be generated by signer from a message M by the following or an equivalent sequence of steps:

1. Select a valid private key s and its associate set of domain parameters for the operation.
2. If the selected signature primitive is
3. Use the dividing operation of the selected message division method to produce a pair cM and vM from the message M .
4. Apply the selected signature primitive to cryptographic portion cM , verification portion vM and private key s , to obtain a signature (c,d) . (Use the selected encryption method, message encoding method, and mask generation function.)
5. Output the signature.

Conformance region recommendation: A conformance region should include:

- At least one valid set of domain parameters
- At least one valid private key s for each set of domain parameters
- A range of messages M

10.5.3 Signature Verification (and Recovery) Operation (new for D2)

A signature (c,d) with a verification portion vM of some message shall be verified by a verifier and the message M recovered by the following or an equivalent sequence of steps:

1. Obtain the other party's purported public key w' and its associated set of domain parameters for the operation.
2. (*Optional.*) Validate the public key w' and its associated set of domain parameters. Output "invalid" and stop if the validation fails.
3. If the selected primitive
4. Apply the selected recovery primitive to the signature (c,d) , the verification portion vM of the message, the signer's public key to recover an octet string cM (the cryptographic portion of the message), or "invalid". If the output of the primitive is "invalid", then stop and output "invalid".
5. Confirm whether or not cM meets the selected redundancy criteria. If not, stop and output "invalid".

6. Use the recovery operation of the selected message division method to recover the message M , from cM and vM .

Conformance region recommendation: A conformance region should include:

- At least one valid set of domain parameters
- At least one valid public key w for each set of domain parameters; if key validation is performed, invalid public keys w that are appropriately rejected by the implementation may also be included in the conformation region
- All the messages M that can be input to the implementation
- All purported signatures (c,d) that can be input to the implementation; this should include at least all (c,d) such that c and d is in the range $[1, r - 1]$, where r is from the domain parameters of the signer's public key

12 Message Encoding Methods

12.3 Message Encoding Methods for Signatures with Message Recovery

12.3.2 EMSR2 (new for D2)

EMSR2 is an encoding method for signatures with message recovery based on the Pintsov-Vanstone Signature Scheme with Message Recovery (PVSSR) [PV99]. It is recommended for use with DL/ECPVSSR.

The method is parameterized by the following choices:

- A non-negative integer $cLen$
- A symmetric encryption method Sym

NOTE— This method does not invoke the method Sym , but rather produces output which valid plaintext for Sym .

12.3.2.1 Encoding Operation

Input:

- The maximum length l of the output
- A cryptographic portion of a message, which is an octet string cM of length $cmLen < 2^{64} - 1$

Output: an octet strings f , which is compatible Sym .

The octet string f shall be computed by the following or equivalent sequence of steps:

1. Encode $cmLen$ as an octet string of four octets, with I2OSP
2. Compute a minimal integer $padLen$ such that $4+cmLen+padLen$ is a valid plaintext length (in octets) for the selected symmetric encryption method Sym .
3. Let $f = cmLen || cM || Z$, where Z is the octet string of $padLen$ 00-valued octets

12.3.2.2 Decoding Operation

Input:

- An octet string f of length $fLen$, which is a valid plaintext of Sym

Assumptions: $fLen \geq 4$

Output: A cryptographic portion of a message, which is an octet string cM

The cryptographic portion of a message cM shall be computed by the following or equivalent sequence of steps:

1. Let $fHead$ be the leading four octets of f . Let $fTail$ be the trailing $fLen - 4$ octets of f
2. Let $cmLen$ be the integer obtained from $fHead$ with OS2IP
3. Let cM be the leading $cmLen$ octets of $fTail$

12.4 Message Division Methods for Signatures with Message Recovery

12.4.1 DMSR1 (new for D2)

DMSR1 is a division method for signatures with message recovery, based on the Pintsov-Vanstone Signature Scheme with Message Recovery (PVSSR) [PV99]. It is recommended for use with DL/ECPVSSR.

The method is parameterized by the following choices:

- A non-negative integer $cLen$

12.4.1.1 Dividing Operation

Input:

- A message, which is an octet string M of length $mLen$

Output: a pair of octet strings cM and vM , the cryptographic portion and the verification portion of the message M .

The two portions cM and vM shall be computed by the following or equivalent sequence of steps:

4. Compute $padLen = cLen - mLen$. If $padLen$ is negative, then let $padLen = 0$.
5. Let pM be the octet string formed by concatenating M with $padLen$ octets equal to 00.
6. Let cM be the leading $cLen$ octets of pM .
7. Let vM be the trailing $mLen + padLen - cLen$ octets of pM

12.4.1.2 Recovery Operation

Input:

- a pair of octet strings cM and vM , the cryptographic portion and the verification portion of the message M .

- **Output:** A message, which is an octet string M

The message M shall be computed by the following or equivalent sequence of steps:

4. Let $M = cM // vM$